IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Application of:	Group Art Unit: 2136
Joshua D. Hug	Confirmation No 1315
Application No.: 10/719,674	Examiner: Johnson, Carlton
Filed: November 21, 2003	
For: RIGHTS ENFORCEMENT AND USAGE REPORTING ON A CLIENT DEVICE	

PRE-APPEAL BRIEF REQUEST FOR REVIEW

TO THE COMMISSIONER FOR PATENTS:

In response to the Advisory Action dated October 10, 2008 ("Advisory Action"), and the Office Action dated July 23, 2008 ("Final Office Action"), Applicant requests review of the final rejection in the above-identified application.

Listing of the Claims begins on page 2 of this paper.

Remarks/Arguments begin on page 10 of this paper.

LISTING OF CLAIMS

1. (Previously Presented) A method comprising:

obtaining clear form rights information at a client device, said clear form rights information being associated with content stored at said client device;

obtaining a clear form external integrity hash of first data comprising said clear form rights information and an external key as an integrity secret;

obtaining an internal integrity hash of second data comprising said clear form rights information, said clear form external integrity hash, and an externally inaccessible client device key;

encrypting said internal integrity hash using said externally inaccessible client device key; and

storing the encrypted internal integrity hash on the client device.

2. (Previously Presented) The method of claim 1 wherein obtaining the clear form external integrity hash comprises:

receiving the clear form external integrity hash from a server device.

3. (Previously Presented) The method of claim 1 wherein obtaining the internal integrity hash comprises:

generating the internal integrity hash on the client device.

4. (Previously Presented) The method of claim 1 further comprising storing said clear form external integrity hash on the client device.

5. (Previously Presented) The method of claim 1 further comprising receiving the external key at the client device.

.

6. (Previously Presented) The method of claim 2 wherein said external key comprises a server device key.

7. (Canceled)

8. (Original) The method of claim 1 further comprising:

receiving, at the client device, a content key for the content;

encrypting the content key using the client device key to generate an encrypted content key; and

storing the encrypted content key on the client device.

9. (Previously Presented) The method of claim 1 further comprising:

generating a validation hash from at least the clear form rights information;

decrypting the encrypted internal integrity hash to recover the internal integrity hash; and

comparing the validation hash to the internal integrity hash to detect tampering with the rights information.

10. (Original) The method of claim 9 further comprising:

disabling the content on the client device if tampering is detected.

11. (Previously Presented) The method of claim 1 further comprising:

storing the clear form rights information on the client device.

12. (Previously Presented) The method of claim 10 further comprising:

reading the clear form rights information from the client device to a server device.

13. (Previously Presented) The method of claim 1 wherein the clear form rights information comprises usage information, the method further comprising:

tracking usage of the content;

updating the clear form rights information with changes in usage; and

for each update of the clear form rights information:

re-obtaining the internal integrity hash of second data comprising the updated clear form rights information, said clear form external integrity hash, and said externally inaccessible client device key; and

re-encrypting, and re-storing the internal integrity hash on the client device .

14. (Previously Presented) The method of claim 1 wherein the internal integrity hash comprises a Hash Message Authentication Code (HMAC).

15. (Original) The method of claim 1 wherein the client device key comprises a code embedded in hardware of the client device having no externally accessible data path.

16. (Original) The method of claim 1 wherein the client device comprises at least one of an MP3 player, a personal data assistant, and cellular phone.

17. (Previously Presented) The method of claim 1 further comprising at least one of:

downloading the clear form rights information from a server device; and

installing a storage medium having the clear form rights information stored thereon.

18. (Previously Presented) The method of claim 1 wherein the clear form rights information grants unlimited play for the content on the client device.

19. (Original) The method of claim 3 wherein generating the internal integrity hash comprises generating the internal integrity hash in trusted hardware.

20-30. (Canceled)

31. (Previously Presented) A method comprising:

generating a validation hash from validation data comprising stored clear form rights information associated with content stored on a client device;

decrypting an encrypted hash to recover an integrity hash using an externally inaccessible client device key , said integrity hash having been previously generated from data comprising the stored clear form rights information and a clear form hash of at least the clear form rights information; and

comparing the validation hash to the integrity hash to detect tampering with the clear form rights information.

32. (Original) The method of claim 31 further comprising:

disabling the content on the client device if tampering is detected.

33. (Original) The method of claim 31 further comprising:

receiving a usage request for the content stored at the client device, said usage request to initiate generation of the validation hash and comparison to the integrity hash; and

permitting usage only if the content is not disabled.

34. (Previously Presented) A client device comprising:

a register operative to store a client device key, said register being externally inaccessible from the client device;

a memory operative to store content and clear form rights information associated with the content, said memory being externally accessible;

hash circuitry operative to:

obtain a clear form external integrity hash of first data comprising the clear form rights information and an external key as an integrity secret; and

obtain an internal integrity hash of second data comprising the clear form rights information, the clear form external integrity hash, and the externally inaccessible client device key; and

encryption circuitry operative to encrypt the internal integrity hash using the client device key ;

said memory being further operative to store the encrypted hash.

35. (Previously Presented) The client device of claim 34 wherein the hash circuitry is operative to obtain the clear form external integrity hash from a server device.

36. (Previously Presented) The client device of claim 34 wherein the hash circuitry is operative to generate the internal integrity hash on the client device.

37. (Canceled) .

38. (Previously Presented) The client device of claim 34 , said memory being further operative to store the clear form external integrity hash .

39. (Previously Presented) The client device of claim 35 wherein the external key comprises a server device key. .

40. (Canceled)

41. (Previously Presented) The client device of claim 34 wherein the encryption circuitry is further operative to encrypt a content key for the content using the client device key ; and the memory is further operative to store the encrypted content key on the client device.

42. (Previously Presented) The client device of claim 34 wherein

the hash circuitry is operative to generate a validation hash from at least the clear form rights information; and

the encryption circuitry is further operative to decrypt the encrypted hash to recover the internal integrity hash;

the client device further comprising:

a comparator to compare the validation hash to the internal integrity hash to detect tampering with the clear form rights information.

43. (Original) The client device of claim 42 further comprising:

a content controller to disable the content on the client device if tampering is detected.

44. (Canceled)

45. (Previously Presented) The client device of claim 34 wherein the rights information comprises usage information, the client device further comprising:

tracking circuitry to track usage of the content and update the clear form rights information with changes in usage;

wherein the hash circuitry and the encryption circuitry are further operative to regenerate, re-encrypt, and re-store the internal integrity hash in the memory for each update of the rights information.

46. (Original) The client device of claim 34 wherein the client device comprises at least one of an MP3 player, a personal data assistant, and cellular phone.

47. (Previously Presented) The client device of claim 34 further comprising at least one of:

an input port to download the clear form rights information from a server device; and

a storage medium port to receive a storage medium having the clear form rights information stored thereon.

48. (Original) The client device of claim 47 wherein the memory at least partially comprises the storage medium.

49. (Previously Presented) A machine readable medium having stored thereon machine executable instructions, the execution of which to implement a method comprising:

receiving clear form rights information at a client device, said rights information being associated with content stored on the client device, said client device having a client device key that is externally inaccessible from the client device;

storing the clear form rights information on the client device ;

obtaining a clear form external integrity hash of first data comprising the clear form rights information and an external key as an integrity secret;

obtaining an internal integrity hash of second data comprising said clear form rights information, said clear form external integrity hash, and an externally inaccessible client device key;

encrypting the internal integrity hash using the externally inaccessible client device key ; and

storing the encrypted internal integrity hash on the client device.

50. (Previously Presented) The machine readable medium of claim 49 wherein obtaining the integrity hash comprises:

receiving the clear form external integrity hash from a server device.

51. (Previously Presented) The machine readable medium of claim 49 wherein obtaining the internal integrity hash comprises: generating the internal integrity hash on the client device.

52. (Previously Presented) The machine readable medium of claim 49 further comprising storing said clear form external integrity hash on the client device. c

53. (Canceled)

54. (Previously Presented) The machine readable medium of claim 50 wherein said external key comprises a server device key.

55. (Canceled)

56. (Original) The machine readable medium of claim 49 wherein the method further comprises:

receiving, at the client device, a content key for the content;

encrypting the content key using the client device key to generate an encrypted content key; and

storing the encrypted content key on the client device.

57. (Previously Presented) The machine readable medium of claim 49 wherein the method further comprises:

generating a validation hash from at least the clear form rights information;

decrypting the encrypted internal integrity hash to recover the internal integrity hash; and

comparing the validation hash to the internal integrity hash to detect tampering with the clear form rights information.

58. (Original) The machine readable medium of claim 57 wherein the method further comprises:

disabling the content on the client device if tampering is detected.

59. (Previously Presented) The machine readable medium of claim 49 wherein the clear form rights information grants unlimited play for the content on the client device.

60. (Previously Presented) The machine readable medium of claim 59 wherein the method further comprises:

reading the clear form rights information from the client device out to a server device.

61. (Previously Presented) The machine readable medium of claim 49 wherein the clear form rights information comprises usage information, the method further comprising:

tracking usage of the content;

updating the clear form rights information with changes in usage; and

for each update of the clear form rights information:

re-obtaining the internal integrity hash of second data comprising the updated clear form rights information, said clear form external integrity hash, and said externally inaccessible client device key; and

re-encrypting, and re-storing the internal integrity hash on the client device.

35 U.S.C. § 103 Rejections

The Office Action concluded that Claims 1-4, 8, 9, 11-19, 31, 34-36, 38, 39, 41, 42, 45-52, 54, 56, 57, 59, and 61 are unpatentable over Published U.S. Patent Application No. 2003/0046238 to Nonaka et al. (hereinafter "*Nonaka*") in view of U.S. Patent No. 7,062,500 to Hall et al. (hereinafter "*Hall*") in further view of U.S. Patent Application No. 2002/0152393 to Thoma et al (hereinafter "*Thoma*"). Claims 5 and 6 were rejected under 35 U.S.C. § 103 as unpatentable over *Nonaka*, *Hall*, and *Thoma* in view of U.S. Patent No. 6,959,384 to Serret-Avila et al. (hereinafter "*Serret-Avila*"). Claims 10, 32, 33, 43, and 58 were rejected under 35 U.S.C. § 103 as unpatentable over *Nonaka*, *Hall*, and *Thoma* in view of U.S. Patent No. 7,080,043 to Chase, Jr. et al. (hereinafter "*Chase*").

Applicant respectfully disagrees. In so asserting, Applicant hereby preserves all other arguments and assertions in the record but respectfully calls the panel's attention to two specific errors. First, the Office Action failed to cite references teaching or suggesting the elements of an internal hash, an external hash, and specific contents of those hashes as recited in Claims 1 and all other claims with similar elements. Second, the Office Action's combination of numerous references was likely based on impermissible hindsight reasoning.

The prior art references clearly do not recite all the elements of Claim 1

Applicant submits that it was clearly erroneous for the Office Action to conclude that the combination of *Hall*, *Nonaka*, *Thoma*, and *Serret-Avila* teaches or suggests every element of Claims 1 and those claims reciting similar elements.

At the outset, the elements of Claim 1 bear repeating here. Claim 1 claims a method that includes "obtaining a **clear form external integrity hash** of **first data**," and claims as another element, "obtaining an **internal integrity hash** of **second data**." In addition to claiming elements with two different hashes, Claim 1 also includes details about the contents of those hashes. Specifically, the contents of the internal hash comprise "said **clear form rights information**, said **clear form external integrity hash**, and **an externally inaccessible client device key**." Moreover, the contents of the external integrity hash of first data comprises "**clear**

form rights information" as well as "an **external key as an integrity secret**." None of the references, alone or in combination, discloses this combination of elements.

First, even a plain reading of the combination of *Hall*, *Nonaka*, and *Thoma* do not support a rejection of Claim 1 under 35 U.S.C. § 103 because they clearly do not teach or suggest, alone or in any combination, two distinct sets of hashes: a clear form external integrity hash and an internal integrity hash. Second, *Hall*, *Nonaka*, and *Thoma* in any combination not only fail to teach or suggest both an internal and external hash, but they also fail to teach the contents of those hashes. Specifically, the prior art fails to teach or suggest the notion of a clear form external integrity hash whose contents also comprise "**an external key as an integrity secret**." Similarly, the prior art fails to teach or suggest an internal integrity hash comprising, *inter alia*, the "**clear form rights information**," a reference to the "**clear form external integrity hash**," and "an **externally inaccessible client device key**."

For example, while the Office Action reasoned that *Hall* disclosed the general concept of "usage of clear form rights information plus . . . using a cryptographic hash," Applicant respectfully submits that it was clearly erroneous to conclude that such a general concept leads to a teaching or suggestion of the elements of Claim 1. For example, it was clearly erroneous to conclude that *Hall's* "usage of clear form rights information" could teach or suggest "obtaining a clear form external integrity hash of first data comprising said **clear form rights information** and an **external key as an integrity secret**." *Hall's* general statements, alone or in combination with the prior art, contain no teaching or suggestion whatsoever of a hash that contains a clear form external integrity hash, let alone an external key as an integrity secret.

Similarly, clearly erroneous generalizations were drawn by the Office Action from *Thoma*. For example, the Office Action at 3 cites to *Thoma* for the proposition that *Thoma* teaches or suggests an inaccessible key thereby rendering Claim 1 obvious. However, *Thoma* merely discloses a "terminal device . . . equipped with [a] unique private key." Thus, it was clearly erroneous to conclude that *Thoma* alone or in combination teaches or suggests "an externally inaccessible client device key" that comprises part of the contents of an "internal integrity hash" as claimed in the language of Claim 1.

Thus, the cited reference clearly fails to disclose all the elements of Claim 1. Accordingly, Applicant submits that it was erroneous to conclude that any combination of *Hall*, *Nonaka*, and *Thoma* renders Claim 1 obvious.

Applicant also respectfully submits that Claims 2-4, 8-9, 11-19, 31, 34-36, 41-42, 44-52, 54, 56-57, 59, and 61, which include elements similar to those discussed above, are allowable at least by similar reasoning and/or by dependency. Similarly, Applicant respectfully submits that Claims 5-6, and Claims 10, 32-33, 43, and 58 are allowable by dependency as well as for the reasons stated in the next section below.

The Office Action clearly erred by employing impermissible hindsight reasoning to support its 35 U.S.C. § 103 rejection.

Applicant respectfully submits that the Office Action employed impermissible hindsight reasoning to arrive at its § 103 rejection of Claims 1-61. In the subsequent Advisory Action, it was asserted that "any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning" and that a "reconstruction" informed by hindsight is proper under some circumstances. Nevertheless, it remains important to avoid the use of improper hindsight reasoning when combining references, *see KSR International Co. v. Teleflex Inc.*, 550 U.S. –, 127 S.Ct. 1727, 1742, and the Federal Circuit has specifically warned of the very species of hindsight reasoning employed by the Office Action when it expressly prohibited "using the applicant's structure as a template and selecting elements from references to fill the gaps," *In re Gorman*, 993 F.2d 982, 18 U.S.P.Q.2d 1885 (1991).

Applicant respectfully submits that only the blueprint provided by Applicant's claims can provide any plausible motivation to pick and choose from among the countless isolated elements from *Nonaka*, *Hall*, *Thoma*, *Serret-Avila*, and *Chase* in the manner asserted in the Office Action. In the interest of expediency, Applicant respectfully requests the panel refer to extended remarks by the Applicant on the subject in Applicant's reply to the Office Action dated September 23, 2008, page 12.

However, two of Applicant's assertions regarding Claim 1 bear repeating here. First relates to the subject matter of the references cited. *Hall* is directed at a method for creating abstract representations of rights management structures. *Thoma* is intended to solve the problem of downloading encrypted data by using a license server. *Nonaka* is directed at a purchasing

method. Finally, *Serret-Avila* is directed at the verification of a hierarchy of digital signatures. Thus, it strains credulity that it would have been obvious to one of ordinary skill in the art, having no familiarity with Applicant's disclosures, to pick out and combine isolated elements from the unrelated references relied on by the Office Action.

Second, the sheer number of references cited supports the Applicant's assertion that hindsight reasoning was employed. The Advisory Action at page 2 asserts that the number of references employed by the Office Action was not "excessive." However, the Office Action cited no less than five different prior art references: a published patent application, *Nonaka*; a patent, *Hall*; a published patent application, *Thoma*; a patent, *Serret-Avila*; and a patent, *Chase*. Accordingly, Applicant respectfully submits that the abundant quantity of references cited by the Office Action is telling of the form of impermissible "blueprint-based" hindsight reasoning employed by the Office Action.

Applicant requests reconsideration and withdrawal of the rejections for the reason that it was clearly erroneous to combine the references as the Office Action did. The remaining claims are also allowable by similar reasoning. Accordingly, Applicant submits that Claims 1-61 are in condition for allowance.

CONCLUSION

Applicant submits that all pending claims are in condition for allowance. Accordingly, early and favorable action allowing all of the pending claims and passing this application to issue is respectfully requested. The Examiner is respectfully requested to contact the undersigned at the telephone number below if there are any remaining questions regarding this application.

We believe the appropriate fees accompany this transmission. If, however, insufficient fee payment or fee overpayment occurs, the amount may be withdrawn or deposited from/to Axios Law Group's deposit account. The deposit account number is 50-4051.

Respectfully submitted,

AXIOS LAW GROUP

Date: October 23, 2008

by: /Adam L.K. Philipp/
Adam L.K. Philipp
Reg. No.: 42,071

AXIOS Law Group
1525 Fourth Avenue, 8th Floor
Seattle, WA 98101
Telephone: 206-217-2200